Securing Collaborative Environments

Deb Agarwal

Keith Jackson and Mary Thompson

Distributed Systems Department
Lawrence Berkeley National Laboratory

2/18/2002

Collaborative Environment Properties

- Users
  - From a diverse set of organizations
  - Many are only occasional participants
  - Each individual needs to be able to participate from a diverse set of locations
  - Heterogeneous access requirements (network and compute platform)
- Composed of many software components
- Dynamic and static resources
- Access permissions dynamically changing
- Often form adhoc

Typical Security Requirements

- Limit participation to authorized people
- Specify and enforce participant access capabilities
- Single sign-on into environment
- Create and enforce authorization policy for dynamic components
- Dynamically change authorization policy
- Identify participant actions (particularly for auditing and logging)

Security Terminology/Mechanisms

- Authentication – identify users
  - PKI Certificates
  - Attribute certificates
  - Username/password
- Authorization – figure out what users are allowed to do
  - Access Control Lists
  - Authorization servers
    - policy
    - capability certificates
- Privacy
  - Private Network (virtual or actual)
  - Encryption
- Data integrity
  - Message Authentication Codes (hash)

Some Existing and Planned Tools

- Grid Security Infrastructure
  - myProxy
- Akenti
- CAS
- Secure Group Communication
- Existing technologies
  - Kerberos
  - SSL/TLS
  - Simple Authentication Security Layer
  - PGP

Grid Security Infrastructure (GSI)

- X.509 Public Key Infrastructure (PKI)-based identity certificates
  - Contains the public key issued and signed by a certificate authority
  - Used with the private key to provide authentication of users (SSL/TLS)
  - A defined set of certificate authorities are trusted to issue identity certificates
- Focuses on control of static resources accessed by a well defined set of users
- Authorization policy is controlled, administered, and enforced at the local resources
  - Grid-mapfile is used to map from identities to local authorization entities
  - Designed to control access to computers

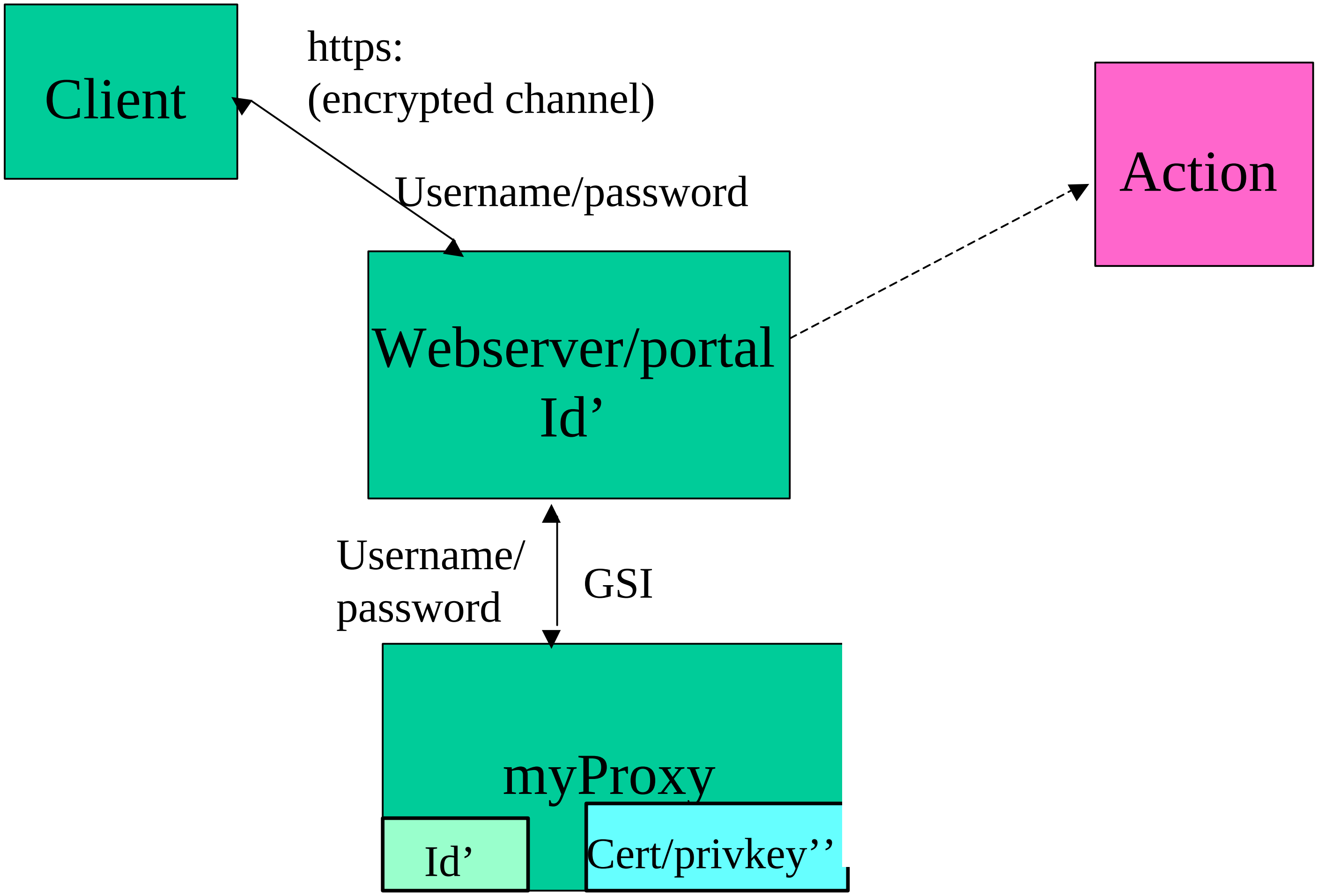
GSI - Proxy Certificates

- Motivation
  - Processes need to be able to act on the user's behalf
  - Do not want to hand the process user's private key
  - Want to support single sign-on
- Proxy certificates derived from the user's identity certificate
- New credential
  - Stored locally unencrypted (no pass phrase)
  - Short-lived (~12-24hrs)
  - Created by calling grid-proxy-init
- Used by processes to act on the user's behalf

GSI - Proxy Service (myProxy)

- Motivation
  - Using proxy credentials requires having access to them
  - Need somewhere to keep proxy credentials
- What is it
  - Repository for proxy credentials
  - Run on a secure (accessible) server machine
- How does it work
  - Stores proxy credentials protected by a password
  - User can unlock using password rather than having a private key
  - Provides proxy credential to processes on your behalf

An Example Use of myProxy



Akenti Authorization

- X.509 or proxy certificates identify user
- Policy is kept in distributed signed certificates
- Policy language allows for access by groups, individuals, possession of arbitrary attributes, run-time constraints such as time-of-day, IP address.
- Policy is written by stakeholders who are defined on a per-resource level.
- Authorization checks are done by a call from the resource gatekeeper to an Akenti server.

Akenti Status

- Used by the Diesel Combustion Collaboratory for control of Web and CORBA accessed resources.
- Will be used by the National Fusion Collaboratory for data access, and code execution access.
- Several tools are provided for the stakeholders to use when creating and viewing policy.
- All access requests to the Akenti server are logged for real-time display and to create an audit log.
- Distributions are available for RedHat Linux and Solaris platforms at http://www.itg.lbl.gov/Akenti

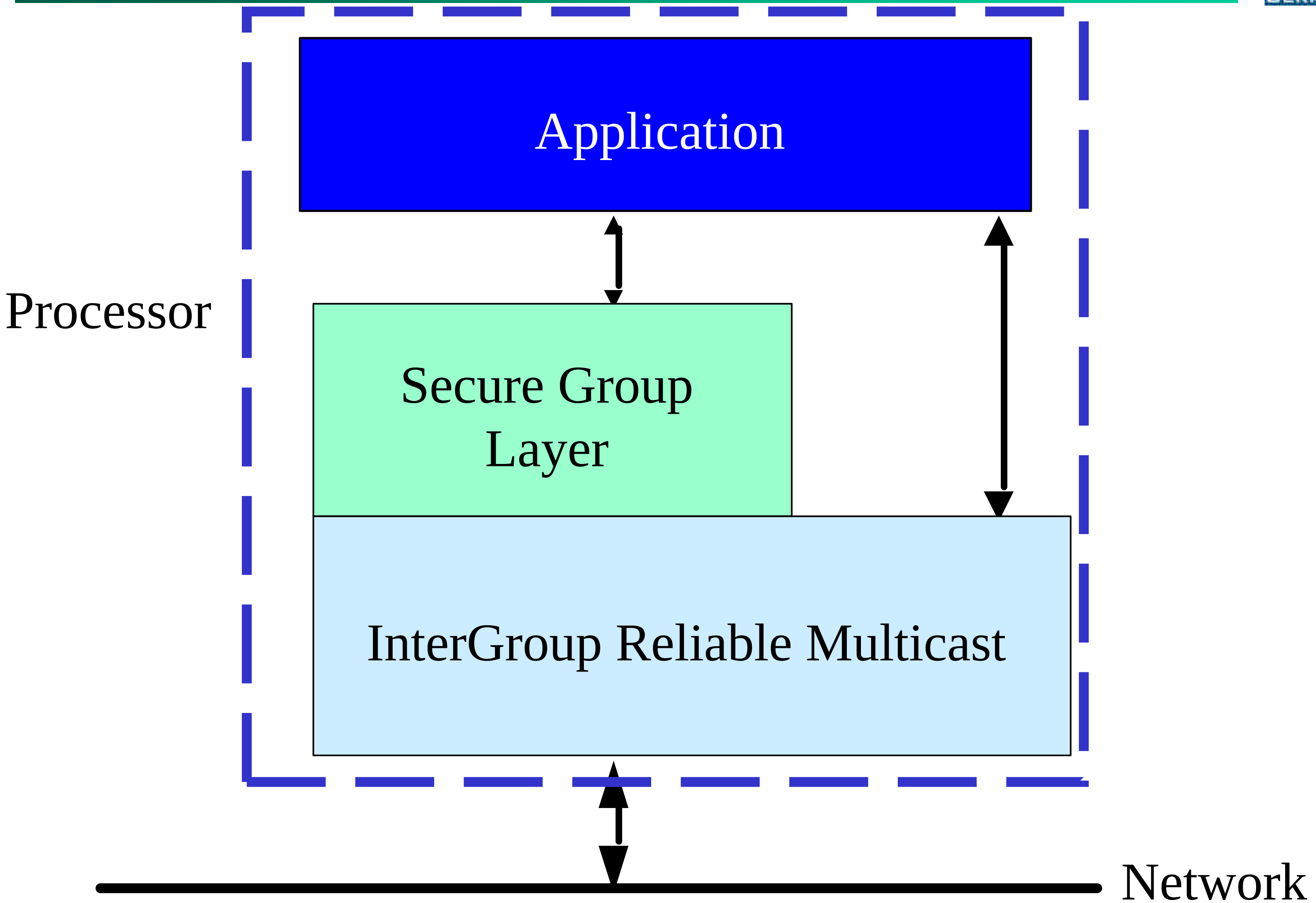
Secure Group Communication

- Secure reliable communication for collaborating groups spread across the Internet
  - simplify communication between components in distributed applications
  - security services similar to SSL/TLS
  - support confidentiality and data integrity
  - support access control based on membership authorization (individually enforced)
  - security services optional

Peer-to-Peer Model

- Allow ad-hoc and dynamic collaboration
- Remove centralized servers
  - scalable to large collaborations
  - remove bottleneck
- Better model for many collaborations – no central authority
- Easy to add new resources to the collaboration
  - minimize setup required
  - allows local control over resource authorization

System Design



Secure Group Layer (SGL)

- Support dynamic membership
  - members join and leave the group at any time (e.g., network partitions and merges)
  - membership is not known in advance
- Achieve strong security goals
  - authenticated key exchange (AKE)
  - mutual authentication (MA)
  - forward secrecy (FS)
- Provide an SSL-like secure channel
- For more information

  http://www-itg.lbl.gov/CIF/GroupCom

What Does It Take To Do PKI

- PKI-based infrastructure
  - What infrastructure do I need to have
    - Certificate Authority/Registration authority - designated entity(s) that verify identities, issues and stores certificates
    - Authorization capability from every resource
      - Authorization server + enforcer
      - Access Control Lists (ACL) + enforcer
  - Issues
    - Users have to manage private keys
    - Cross-domain authentication
    - Revocation
    - Authorization management
      - changes
      - Scalability
    - High infrastructure and trust threshold for entry

Password + PKI + Proxy

- Username/password
  - Provides new users with a means of quick access
  - Allows users to participate from untrusted sites
  - Support adhoc collaborations
- PKI
  - Support the core users and protect critical resources
- Proxy service
  - Provide PKI users with a way to use their PKI credentials via a password
  - Mechanism for single sign-on

Issues

- Unique identities
- Mechanisms to bootstrap environment
- What is the trust entity and how do you build trust incrementally
- ….

What Can We As ACE Do?

- Best practices document identifying methods of securing collaboratories (e.g.)
  - Deploying PKI-based collaborative software
  - Using proxies to secure collaborative software
- Identify missing capabilities
  - Dynamic authorization mechanisms
  - Incremental trust building mechanisms
  - Distributed certificate authorities (cross-organization trust)